HEALTH AFFAIRS

TRICARE
Management
Activity

HIPAA RISK MANAGEMENT ACTIVITIES

Version 2.0

TMA Privacy Office

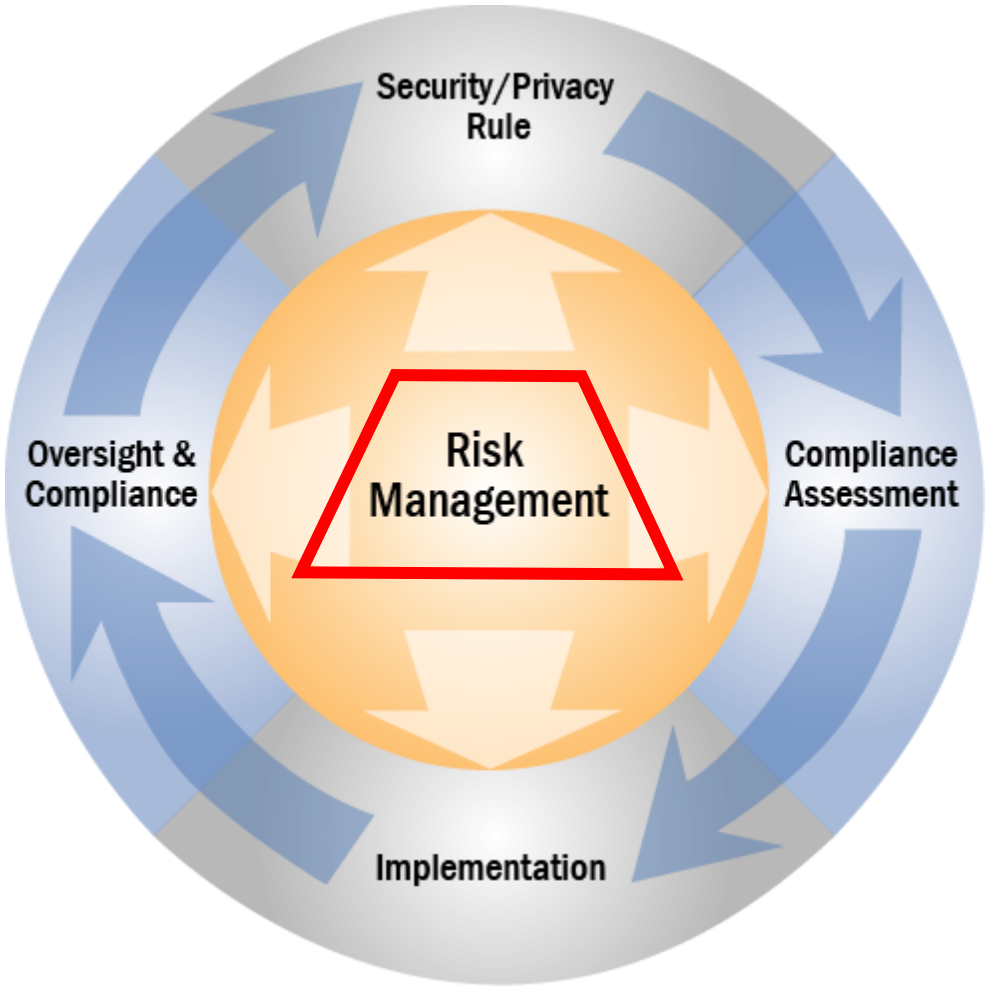
Agenda

- Information Security Concepts
- Risk Assessment
- Risk Mitigation
- Risk Monitoring

Objectives

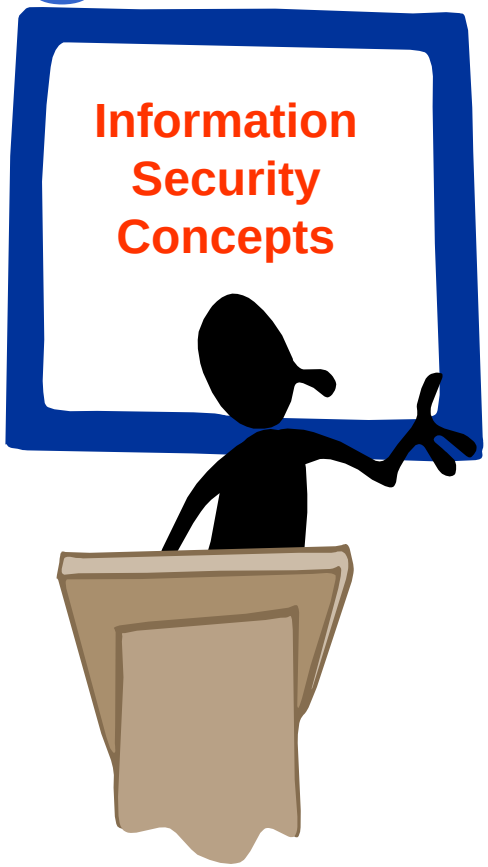
- After completing this course, you should be able to:
  - Define basic information security concepts
  - Describe the elements of the risk management process
  - Identify the risk management activities of the HIPAA Security Rule
  - Describe how OCTAVE and HIPAA BASICS support HIPAA compliance

HIPAA Implementation Life Cycle



Information Security Concepts

Objectives



- After completing this module, you should be able to:
  - Define terminology and basic concepts of information security
  - Identify the federal regulatory aspects of information security including laws and guidance

Information Security

Information security is achieved through an integrated system of policies, procedures, products, and people that identify, control, and protect information by an information protection strategy that is authorized by management and integral to good business practice.

Legislative Requirements

- Federal laws and regulations require agencies to be accountable for results, and provide security for information and assets
  - Health Insurance Portability and Accountability Act (HIPAA) of 1996
  - Office of Management and Budget (OMB) Circular A-123
  - Computer Security Act of 1987
  - OMB Circular A-130, Appendix III
  - Federal Information Security Management Act (FISMA)
  - Federal Managers Financial Integrity Act of 1982 (FMFIA)
  - Government Performance and Results Act (GPRA)

DoD Requirements

- Federal laws and regulations require agencies to be accountable for results, and provide security for information and assets
  - DoD 5000.1-D, Defense Acquisitions
  - DoD 5000.2-R, Mandatory Procedures for MDAS & MAIS Acquisition
  - DoD 5160.54-D, Critical Asset Assurance Program
  - DoD 5200.2-D, Personnel Security Program
  - DoD 5200.2-R, Personnel Security Program
  - DoD 5200.40-I, DITSCAP
  - DoD 5200.8-D, Security of DoD Installations & Resources
  - DoD 5200.8-R, Physical Security Program
  - DoD 5215.2-I, Computer Security Technical Vulnerabilities Reporting Program
  - DoD 6510.18-R, DoD Health Information Privacy
  - DoD 8000.1-D, Defense Information Management Program

DoD Requirements

- Federal laws and regulations require agencies to be accountable for results, and provide security for information and assets
  - DoD 8000.1-D, Defense Information Management Program
  - DoD 8500.1-D, Information Assurance
  - DoD 8500.2-I, Information Assurance Implementation
  - DoD 8510.1-M, DITSCAP
- Service-specific regulations

Security Goals (1 of 2)

- **Confidentiality** - protecting information from disclosure to unauthorized people or processes

- **Availability** - protecting information and resources from unauthorized or malicious use so the information or resources are accessible when needed

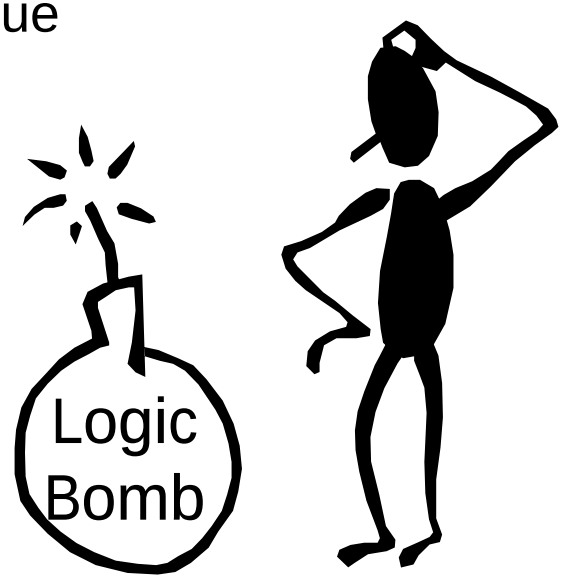
Security Goals (2 of 2)

- **Integrity** - assuring the reliability and accuracy of information and IT resources
- **Authentication -** means for validating a transmission, message or originator
- **Non-repudiation** - providing assurance as to proof of origin and proof of delivery so neither party can deny having processed the data

Threat

- A threat is the potential to cause unauthorized disclosure, changes, or destruction of an asset
  - Unauthorized disclosure = breach of confidentiality
  - Unauthorized changes = integrity failure
  - Unauthorized destruction = availability issue

- Types of threats:
  - Natural
  - Manmade
  - Environmental



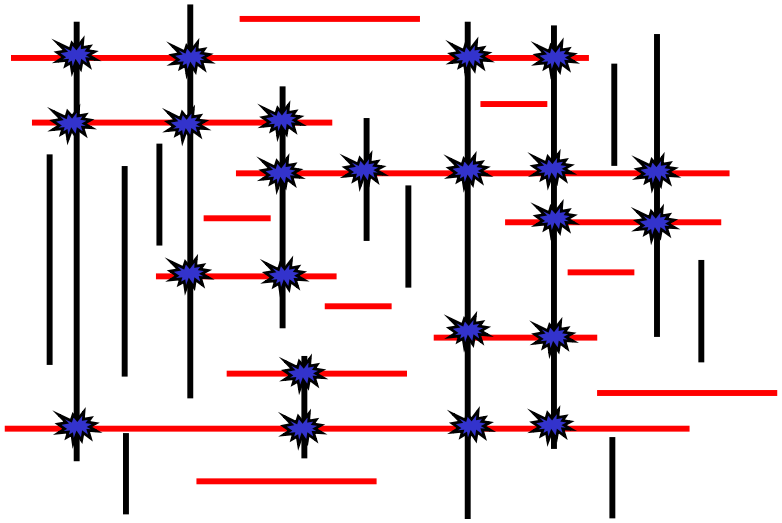
Vulnerability

- Any flaw or weakness that can be exploited and results in a breach or a violation of the organization's security policy

- Types of vulnerabilities:
  - Poorly communicated or implemented policy
  - Poorly trained personnel
  - Misconfigured systems or controls
  - Lack of access controls
  - Lack of physical controls
  - Lack of visitor policy

What is Risk?

- A function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization



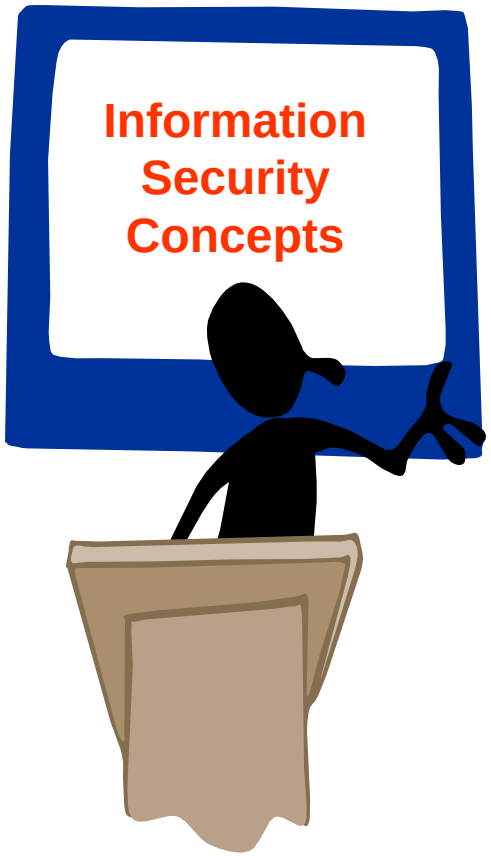
Components of Risk

Security Controls

- Categories
  - Administrative
  - Physical
  - Technical

- Sources
  - DoD 8500.2, Information Assurance Implementation
  - Individual Service Regulations
  - NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
  - NIST SP 800-53, Recommended Security Controls for Federal Information Systems (DRAFT)
  - HIPAA Security Rule

Summary



- You should now be able to:
  - Define terminology and basic concepts of information security
  - Identify the federal and DoD regulatory aspects of information security including laws and guidance

Risk Management

Objectives

- After completing this module, you will be able to:
  - List some recent events that highlight the necessity for good risk management practices
  - Identify the three components of risk management

Recent Events (1 of 3)

- **Computer Virus Damage**

Year	Code Name	Worldwide Economic Impact ($US)
2003	SQL Slammer	$1.0 Billion
2001	Nimda	$653 Million
2001	Code Red(s)	$2.62 Billion
2001	SirCam	$1.15 Billion
2000	Love Bug	$8.75 Billion
1999	Melissa	$1.10 Billion
1999	Explorer	$1.02 Billion

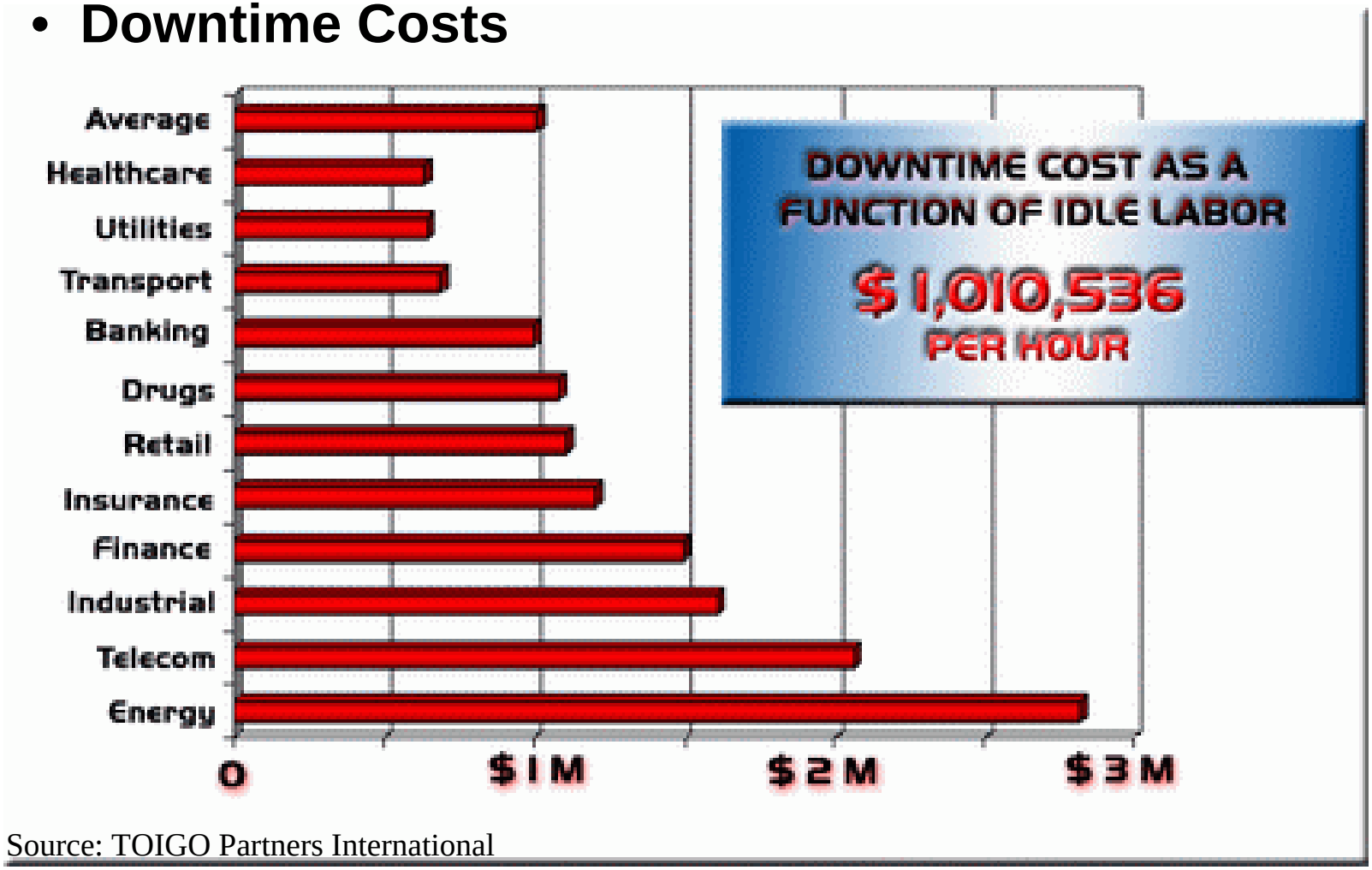
Source: Computer Economics

Recent Events (2 of 3)

- **Identity Theft**
  - 27 Million Americans – last five years
  - 10 Million Americans – last year
  - Business cost - $47.6 Billion
  - Victim cost - $5.0 Billion

Recent Events (3 of 3)

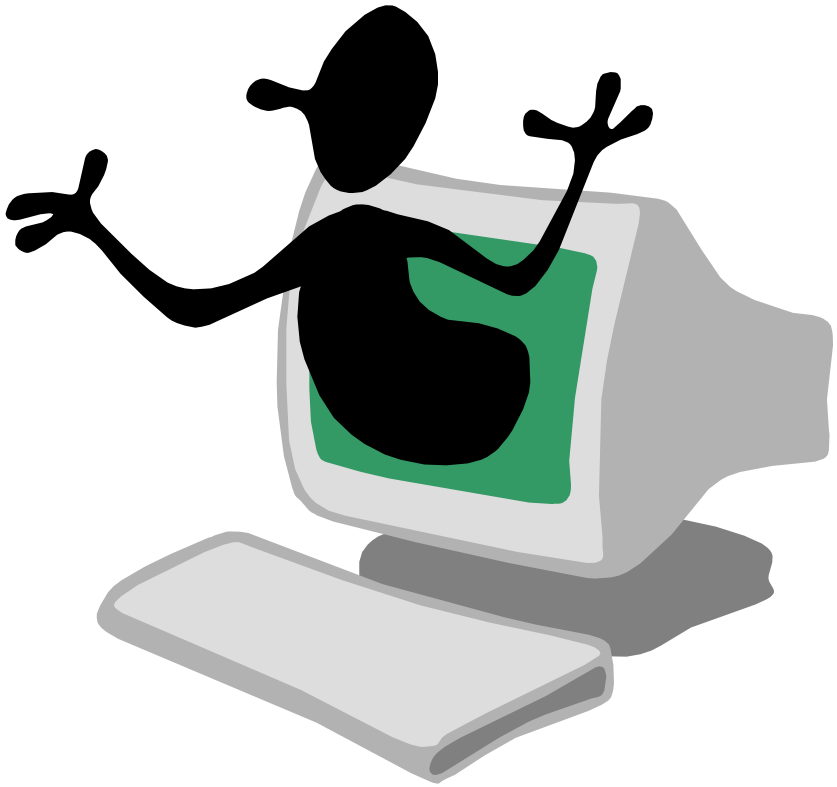
- **Downtime Costs**



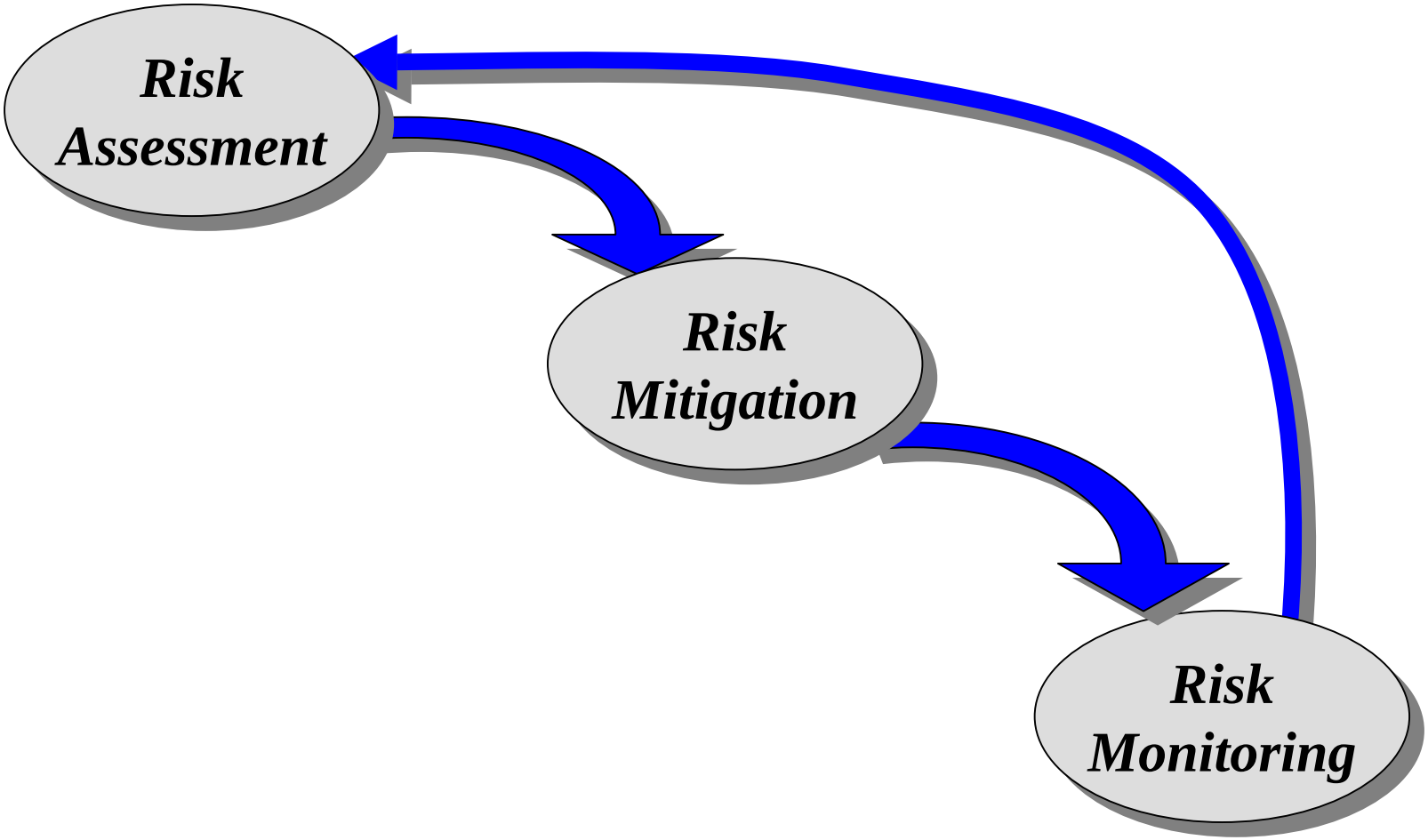
Source: TOIGO Partners International

What is Risk Management?

- Risk Management is composed of three parts:
  - Risk Assessment
  - Risk Mitigation
  - Risk Monitoring



Risk Management Process



Summary

- You should now be able to:
  - List some recent events that highlight the necessity for good risk management practices
  - Identify the three components of risk management

Risk Assessment

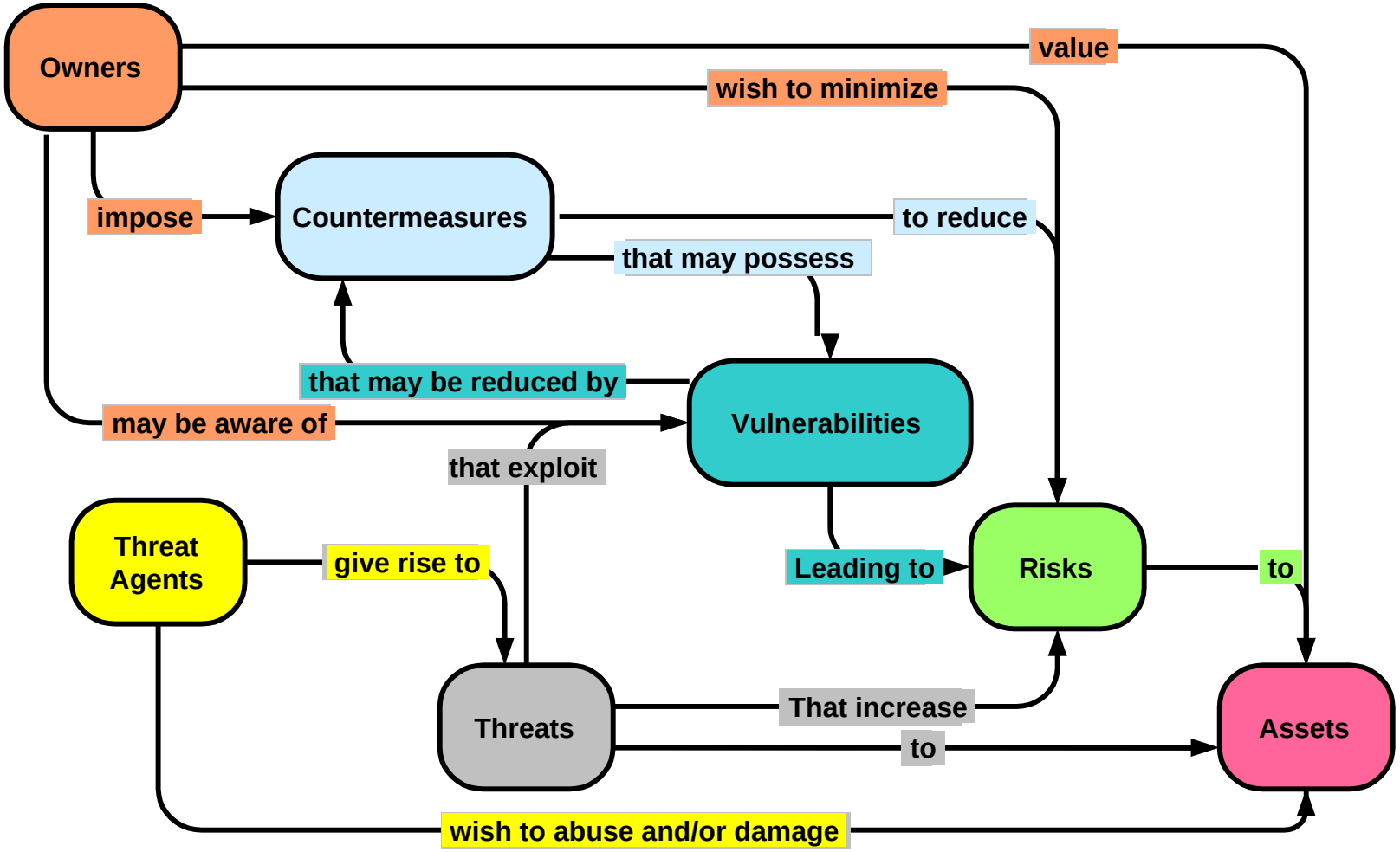
Objectives

- After completing this module, you should be able to:
  - Describe risk assessment
  - Define threats
  - List and describe the nine-steps of the risk assessment methodology

Risk Assessment

- Identification and evaluation of risks and risk impacts
- Recommendations of risk-reducing measures

Risk Assessment Model



Risk Assessment Methodology

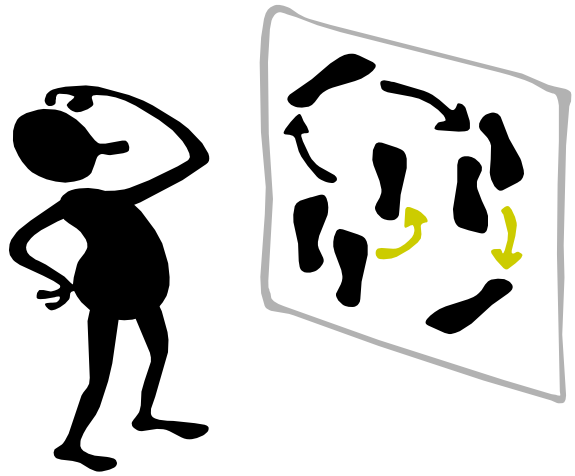
- Provides a straightforward description of the system and a qualitative assessment of the risk (e.g., high, moderate, low)

- Risk assessment is composed of a nine-step systematic process
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact Analysis
  - Risk Determination
  - Control Recommendations
  - Results Documentation

Details of the Process

- Steps indicate a general sequence of activities, but some elements of one activity may be mixed with other activities

- Activities can also be affected by the system development life cycle phase



System Development Life Cycle (SDLC)

- The phase in which the system resides determines the

- Used to assess risk

SDLC Phases (1 of 2)

- Initiation
  - Supports the development of a system security policy and security concept of operations (CONOPs)
- Development and Acquisition
  - Supports the security analyses that lead to architecture and design trade offs
- Implementation
  - Supports the assessment of the system implementation against its requirements and within its modeled operation environment

SDLC Phases (2 of 2)

- Operation and Maintenance
  - Supports analysis of the system's security posture in the true operational environment
  - Well-defined system hardware and software characteristics and vulnerabilities can be specifically defined and in fact, may be well-known
- Disposal
  - Remove and/or archive information
  - Sanitize hardware and software
  - Ensure proper disposal of all devices

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Purpose

- To identify system resources and information that constitute the system and its boundaries, including
  - Hardware
  - Software
  - Biomedical Devices
  - System Interfaces
  - Data and Information
  - People
  - System Mission
- Provides the foundation for the remaining steps of the risk assessment process

Typical Information Sources

- Questionnaires
- Site visits
- Interviews
- Automated scanning tools
- Security documentation
- System and site documentation

System and Site Documentation

- Mission statements
- Concept of Operations
- Security policies and procedures
- System functional requirements
- System architectural design documents
- Site operations manual
- Standard operating procedures
- Reports from previous risk assessments
- Physical security plans
- Site floor maps

Summary

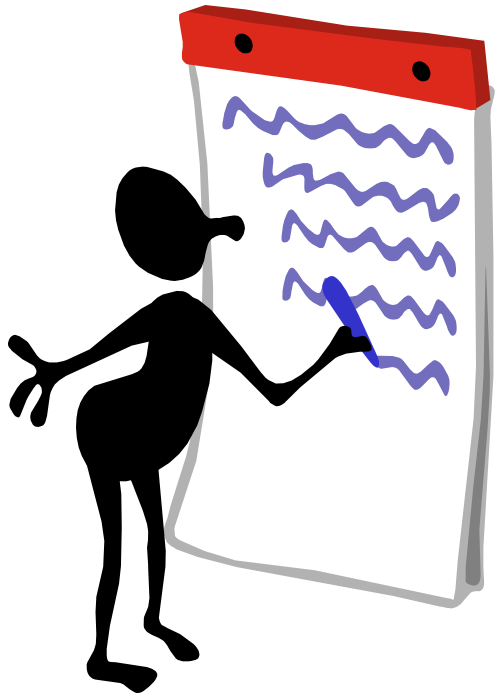
- Purpose of Step One, System Characterization:
  - To identify system resources and information that constitute the system and its boundaries

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Threat Identification

Purpose



- To identify and develop a list of realistic natural, manmade, and environmental threats

Threat Concepts

- Threat
  - The potential to cause unauthorized disclosure, unauthorized modification, or destruction of or denial of access to an asset
- Threat-Source
  - Any circumstance or event with potential to cause harm to an IT system and its assets
  - The common threat-sources can be natural, environmental, or manmade

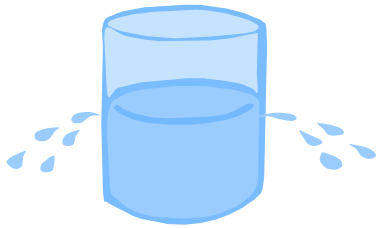
Threat Identification

Threats

- Natural
  - Floods
  - Earthquakes
  - Tornadoes
  - Electrical Storms

- Manmade
  - Disgruntled employee
  - Arson
  - Social Engineering
  - Unintentional alterations

- Environmental
  - Long-term power failure
  - Pollution
  - Chemicals
  - Liquid Leakage



Threat Identification

Assessment of Threat

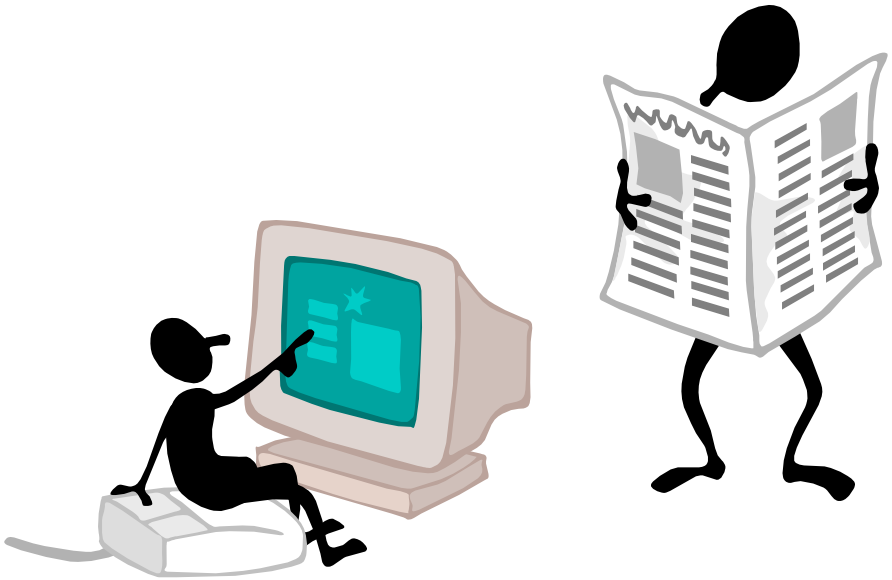
M ~ O ~ M

- Means
- Opportunity
- Motivation – for intentional actions

of your adversaries

Threat Data Sources

- Many sources of data
  - US-CERT
  - DoD-CERT
  - CERT Coordination Center
  - IAVA
  - Mass media
  - sans.org



- NOTE: Simply because a threat is listed does not necessarily mean that the threat can affect the system

Summary

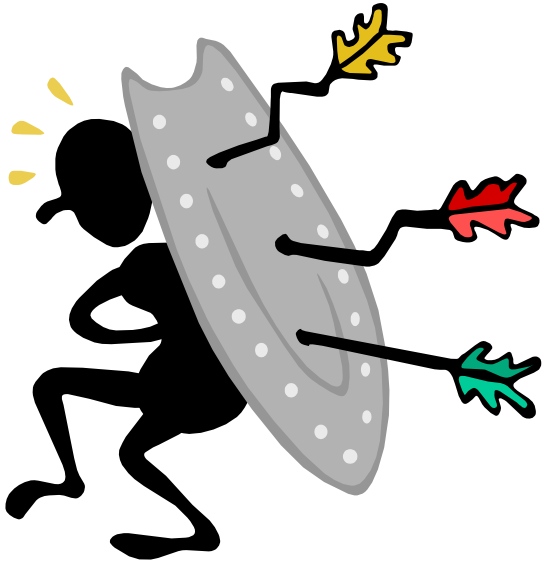
- The outcome of Step 2, Threat Identification will be a threat statement that lists realistic natural and manmade threats and threat agents applicable to the system being evaluated

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Vulnerability Identification

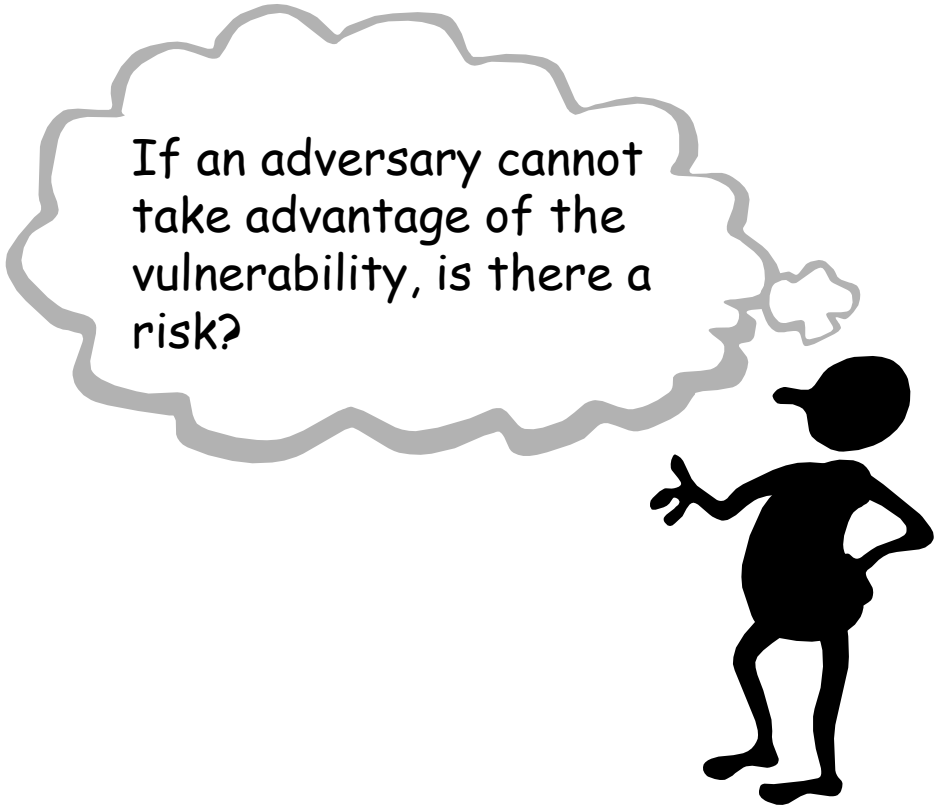
Purpose



- To identify and develop a comprehensive list of possible vulnerabilities that could be used in an attack on the system

What a vulnerability?

- Any weakness that can be exploited to gain access to an asset



Identifying Vulnerabilities

- Physical security
- Computer/technical security
- Communications security
- Personnel security
- Administrative/Management security

Note: Unmet security requirements are vulnerabilities

Vulnerability Identification

Note….

- The phase of the SDLC affects the vulnerability assessment:
  - Initiation

    The primary sources of vulnerabilities are derived from information about the considered or proposed network components, their operating systems and applications
  - Development and Acquisition

    Vulnerability identification expands to include automated tools and databases of known vulnerabilities to identify appropriate system security configurations
  - Operation and Maintenance

    Vulnerability identification includes determining and analyzing implemented security features using:
    - Proactive methods
    - Documented vulnerability sources

Vulnerability Identification

Proactive Methods

- Automated vulnerability scanning
- Network mapping
- Security testing and evaluation
- Penetration testing

Vulnerability Identification

Documented Sources

- Previous risk assessments
- CERT and CIAC bulletins
- Vendor advisories
- Vulnerability listings
- System software security analyses
- System information analyses
- System development test procedures
- System test results
- System anomaly reports

Vulnerability Identification

Also…

- Security requirements collected in Step 1 are reviewed to determine if they are being met by security countermeasures that are either in place or planned

Vulnerability Identification

What do you think?
Threats vs. Vulnerabilities

Threat or Vulnerability	Answer
1. The LAN is not protected by a firewall.	
2. A malicious user could attempt to gain unauthorized access to the system.	
3. A risk assessment has not been conducted every three years.	
4. The operating system (e.g., Windows NT) allows unlimited bad logon attempts.	
5. Motivated threat agents seeking personal profit gain unauthorized access to the LAN.	
6. Authorized users can use system knowledge to circumvent computer security protective measures, exceed their authorized access privileges, and browse confidential files.	
7. An unauthorized user could disclose, alter, or delete critical and sensitive agency information.	
8. Unnecessary services are running on critical servers.	
9. There is no formal process for removing inactive user accounts and terminated employee system access.	
10. The router access control list allows unrestricted access to the LAN.	

Summary

- During Step 3, vulnerabilities that could be used in an attack on the system are identified and developed into a comprehensive list

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Control Analysis

Purpose

- To analyze the controls that have been implemented, or planned for implementation to minimize or eliminate the likelihood of a threat exercising a system vulnerability

Control Analysis

Control Methods

- **Technical** controls are safeguards incorporated into computer hardware, software or firmware
- **Non-technical** controls are administrative and physical controls
  - Security policies
  - Standard operating procedures
  - Physical security
  - Personnel security
  - Environmental security

Control Categories

- Preventive controls inhibit attempts to violate security policy
  - Control enforcement
  - Encryption
  - Authentication
- Detective controls warn of violations or attempted violations of security policy
  - Audit trails
  - Intrusion detection methods
  - Checksums

Control Analysis

Summary

- The output of step 4 is a list of current or planned controls used by the IT system to mitigate the likelihood that a vulnerability will be exercised and reduce the impact of such an adverse event

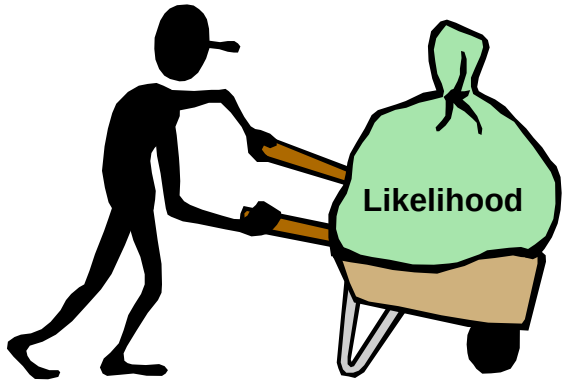
Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Likelihood Determination

Purpose

- To derive an overall likelihood rating of probability that a potential vulnerability may be exercised considering:
  - Threat-source motivation and capability
  - Nature of vulnerability
  - Existence and effectiveness of current controls



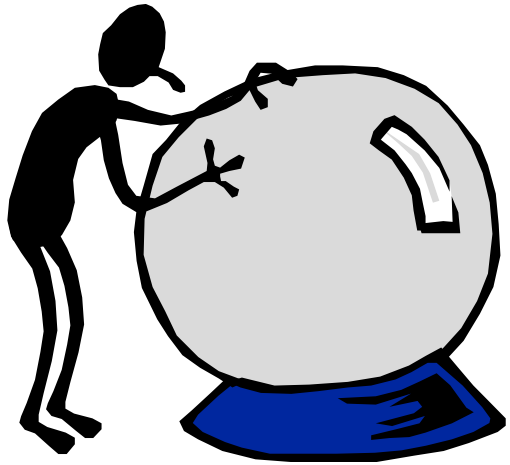
Likelihood Determination

Likelihood Rating

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable and/or controls to prevent the vulnerability are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent or significantly impede the vulnerability from being exercised

Summary

- The output of Step 5 is a likelihood rating, in terms of *high*, *medium*, or *low*, that each identified vulnerability will be exercised by its associated threat



Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Impact Analysis

Purpose

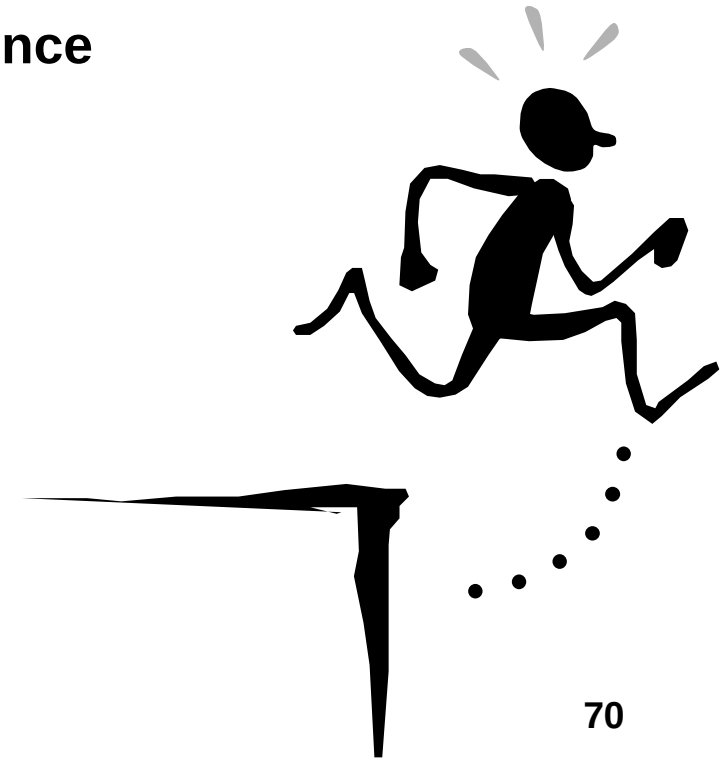
- To determine the adverse impact resulting from a successful threat exercise of a vulnerability
- Information needed for analysis
  - Organization mission
  - System and data criticality
  - System and data sensitivity

Outcome of a Security Event

- **Loss of Integrity** – Unauthorized changes are made to data or IT system (intentional or accidental)
- **Loss of Availability** – May result in loss of productive time impeding the end users' performance of functions supporting the organization's mission
- **Loss of Confidentiality** – Unauthorized disclosure of information may range from jeopardizing of national security to the disclosure of protected health information

Impact of the Outcome

- **Consider the impact to the organization of an unauthorized disclosure, unauthorized modification, unauthorized destruction or denial of access in all of the following areas:**
  - **Reputation and customer confidence**
  - **Life and health of customers**
  - **Productivity**
  - **Fines and legal penalties**
  - **Financial**
  - **Readiness**

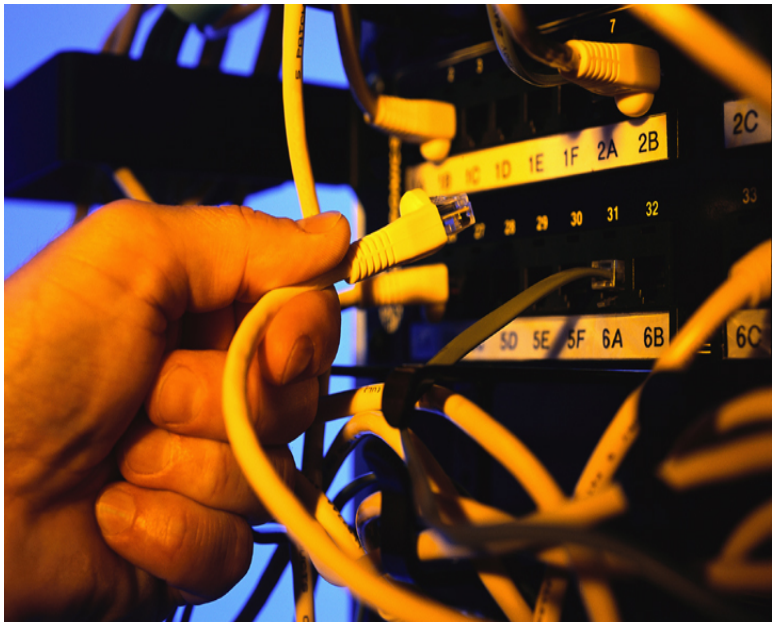


Impacting Business (1 of 3)

- **Tangible Losses - Confidentiality Breach**
  - Loss of intellectual property
  - Consulting/legal fees
  - Public relations
  - Cost of business

Impacting Business (2 of 3)

- **Tangible Losses - Integrity Breach**
  - Data Recovery and Reconstitution Cost
  - Consulting/Legal Fees
  - Loss of User Productivity



Impacting Business (3 of 3)

- **Tangible Losses – Loss of Availability**
  - Decrease in user productivity
  - Loss of business revenue
  - Disaster recovery costs

Impact Analysis

Output

- The output of Step 6 is a magnitude of impact rating, in terms of *high*, *medium*, or *low,* for each threat-vulnerability pair
  - The magnitude of impact rating which can be used in a cost-benefit analysis of recommended controls

Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Risk Determination

Purpose

- To assess the level of risk to the IT systems and the information of the organization
- The determination of risk for a particular threat-vulnerability can be expressed as a function of
  - The likelihood of a given threat source's attempting of exercise a given vulnerability
  - The magnitude of the impact should the threat-source exercise the vulnerability
  - The adequacy of planned or existing security controls for reducing or eliminating risk

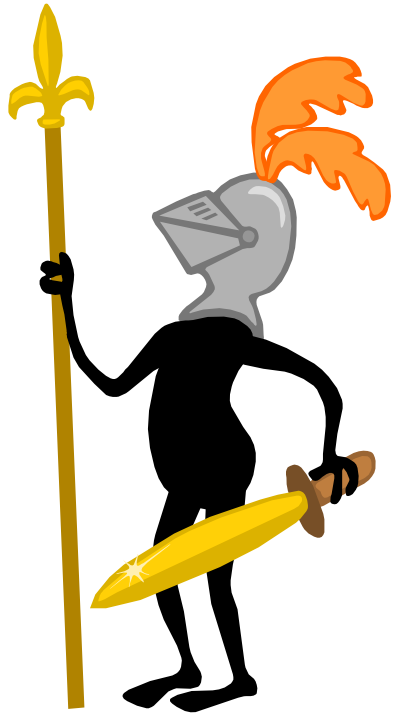
Risk Determination

Risk Scale and Necessary Actions

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be in place as soon as possible
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time
Low	If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk

Output

- The output of step 7 is a risk-level rating for each threat-vulnerability pair
- The rating indicates what actions should be taken to mitigate the risk



Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

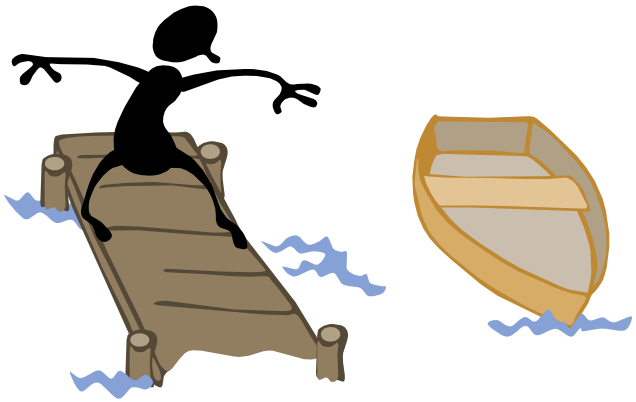
Purpose

- To reduce the level of risk to the IT system and its data to an acceptable level
- Factors in recommending controls and alternative solutions
  - Effectiveness of recommended options
  - Legislation and regulations
  - Organizational policy
  - Operational impact
  - Safety and reliability
  - Cost

Control Recommendations

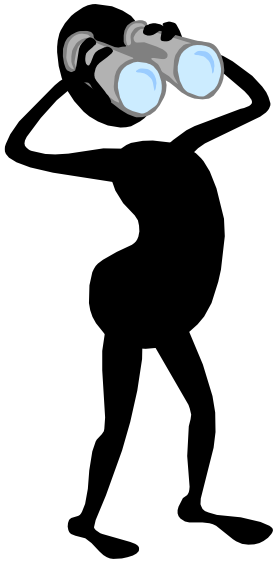
Remember….

- Some solutions may provide multiple services
- Placement of the service is critical
- Need balance between what's appropriate and cost effective



Control Recommendations

Output



- The output of Step 8 is a recommendation of control(s) and alternative solutions to mitigate risk

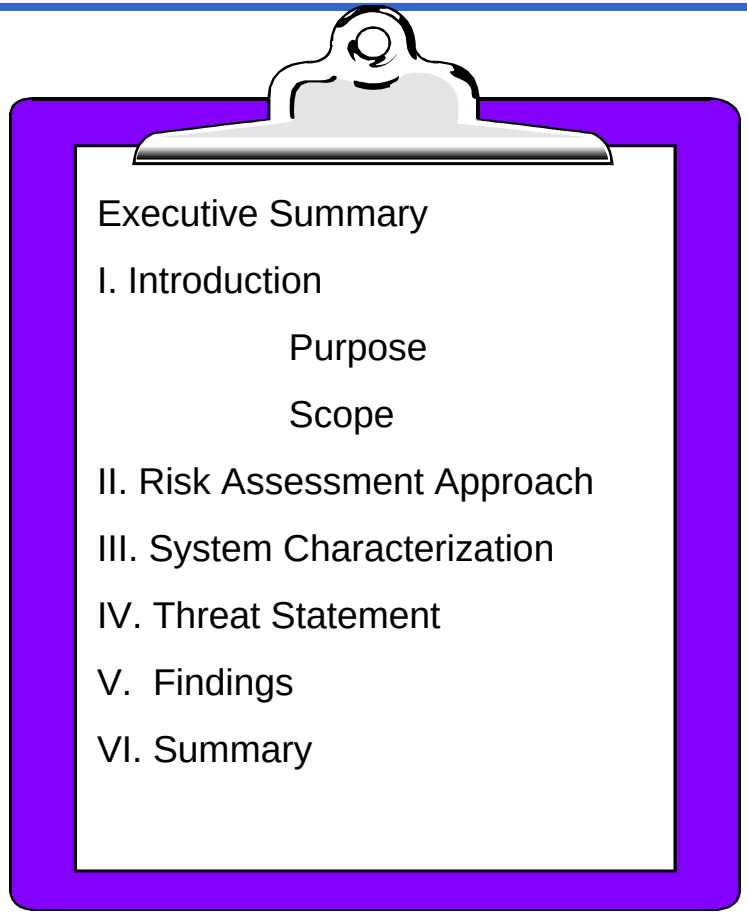
Risk Assessment – Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

Results Documentation

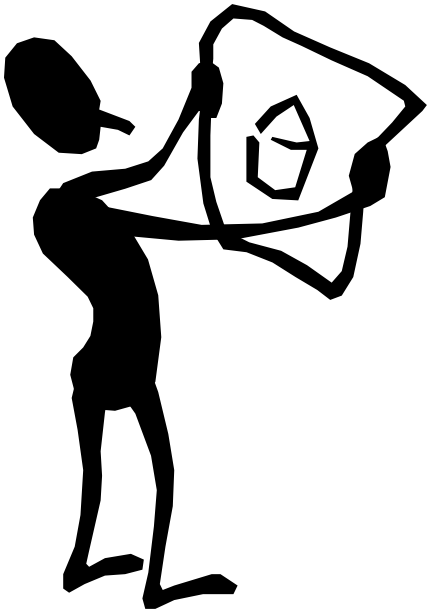
Purpose

- The results of the risk assessment should be documented in a report



Results Documentation

Report Contents



- The risk assessment report should be of sufficient detail to allow the organization's management to make informed decisions on appropriate actions in response to the risks identified

Results Documentation

Risk Assessment Report Outline

- Executive Summary

I. Introduction

II. Risk Assessment Approach

III. System Characterization

IV. Threat Statement

V. Risk Assessment Results

VI. Summary

Risk Assessment Report

Introduction

- Purpose
- Scope
- Describe
  - System Components
  - Elements
  - Users
  - Site locations
  - Other details as necessary

Risk Assessment Approach

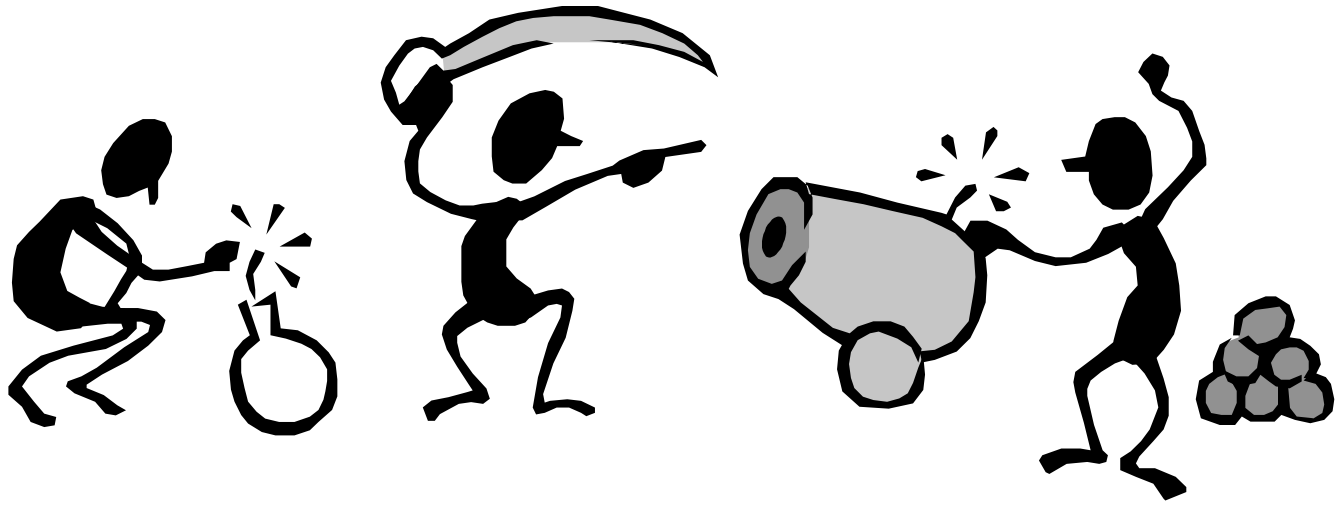
- Describe approach used
  - Risk Assessment Team members
  - Techniques used to gather information (use of tools, questionnaires, etc)
  - Development and description of risk scale (3x3, 4x4, or 5x5 risk level matrix)

System Characterization

- Describe the system
  - Hardware (server, router, switch)
  - Software (application, operating system, protocol)
  - System Interfaces (communication link)
  - Data
  - Users
- Provide connectivity diagram or system input and output flowchart

Threat Statement

- Compile potential threat sources
- List associated threat actions



Risk Assessment Results

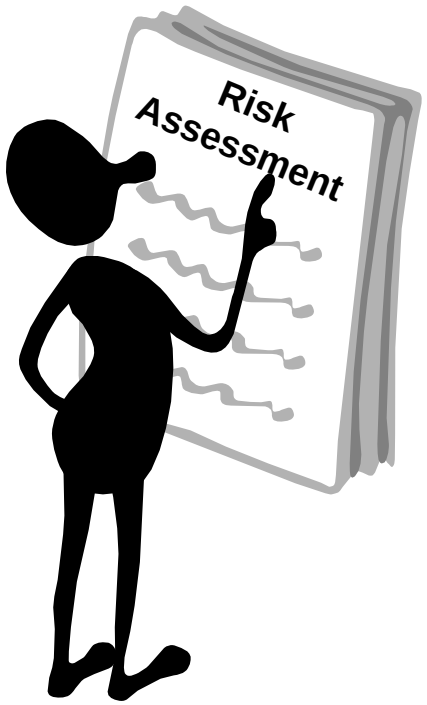
- List observations (vulnerability/threat pairs)
- Observations contain:
  - Observation number and brief description
  - Discussion of threat-source and vulnerability pair
  - Identification of existing mitigation security controls
  - Likelihood discussion and evaluation
  - Impact analysis discussion and evaluation
  - Risk rating
  - Recommended controls or alternative options

Summary

- Total number of observations
- Summarize
  - Observations
  - Associated risk levels
  - Recommendations
  - Any comments
- Organize into a table to facilitate implementation

Results Documentation

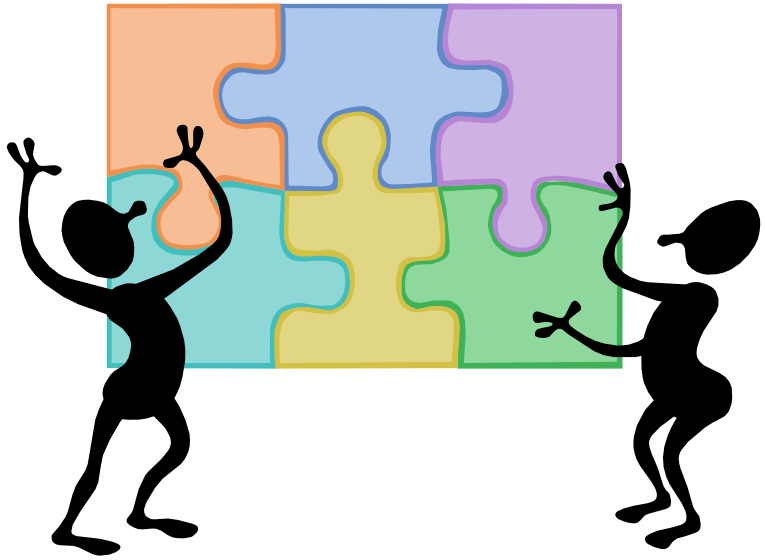
Output



- The output of Step 9 is the completed risk assessment report

The Nine Steps

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact analysis
7. Risk Determination
8. Control Recommendation
9. Results Documentation



What do you think?

- Three kinds of threats are: natural, manmade, and environmental
- Adverse impacts of a security event are loss of integrity, availability, or confidentiality
- The risk assessment report should include enough detail to allow managers to make informed decisions on appropriate actions in response to identified risks

Summary

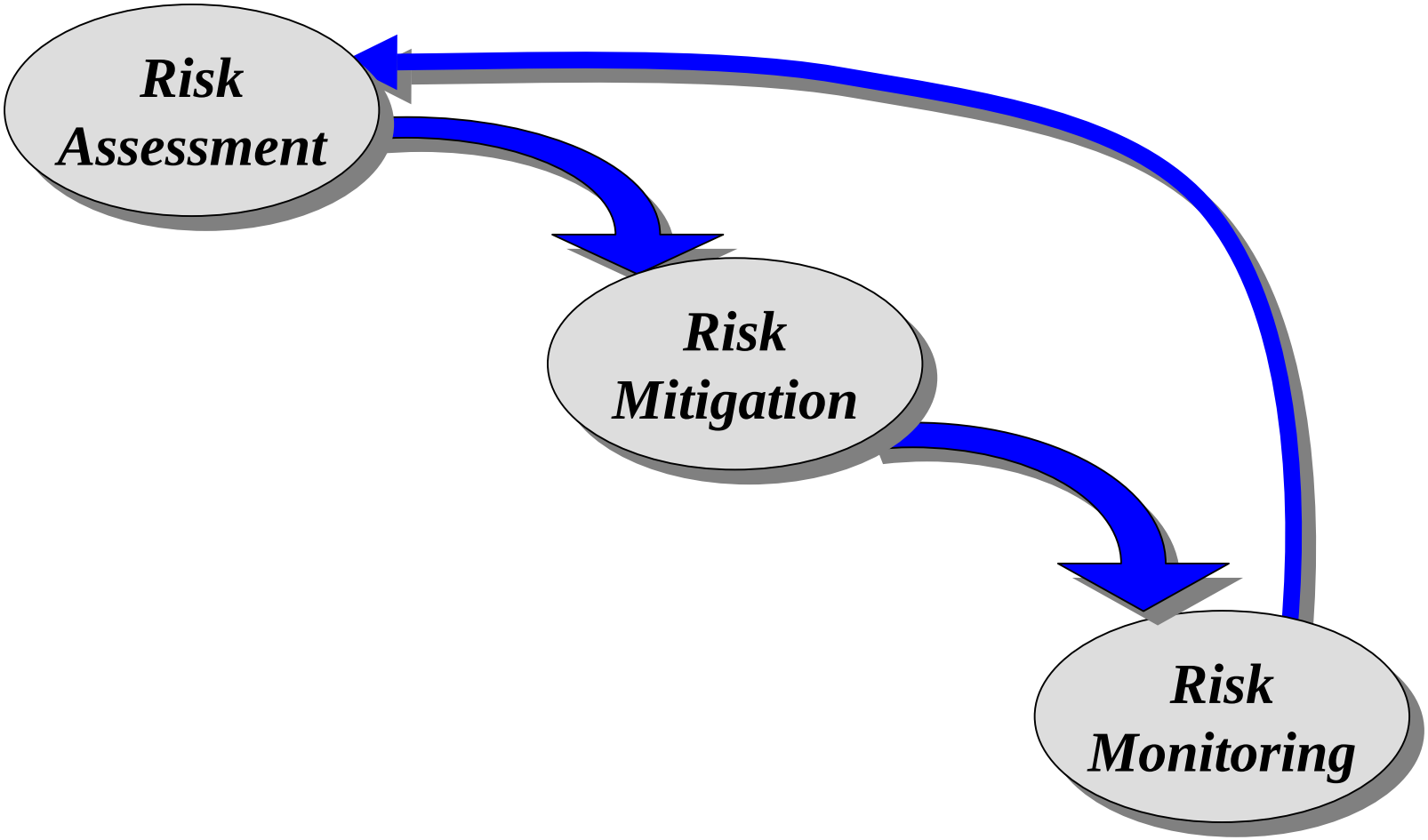
- You should now be able to:
  - Describe risk assessment
  - Define threats
  - List and describe the nine-steps of the risk assessment methodology

Risk Mitigation

Objectives

- After completing this module, you should be able to:
  - Describe the components of risk mitigation
  - List and describe who is involved in the risk mitigation process
  - Describe risk mitigation options

Risk Management Process



What is Risk Mitigation?

- The process of identifying areas of risk that are unacceptable; and estimating countermeasures, costs and resources to be implemented as a measure to reduce the level of risk

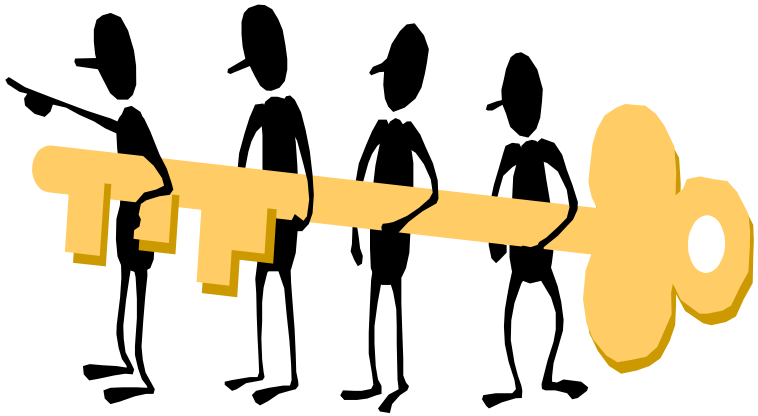
Risk Mitigation

Purpose

- To enable management to make informed decisions regarding countermeasure analysis against known risk to a system(s)

Who is involved?

- Risk determinations are not made in isolation. Decisions must include Management and Business Owners
- Recommended Staff involvement:
  - Executive Council
  - Clinical Representative
  - Business Process Owners
  - Comptroller
  - Billing Office
  - Personnel Office/Human Resources
  - CIO
  - ISSO
  - Patient Administration/Medical Records

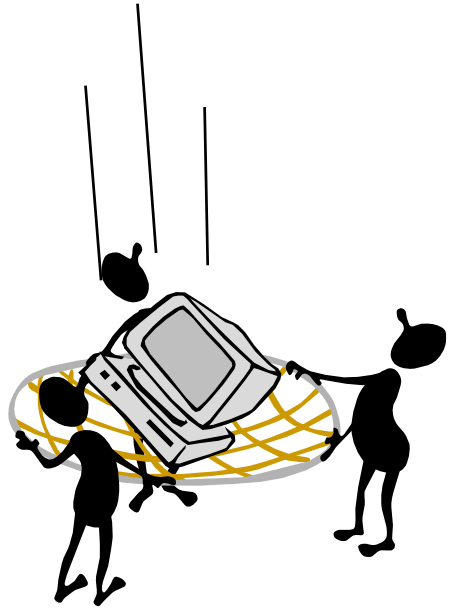


Ultimate Responsibility

- It is the decision of the Commander (DAA) of the facility to assume a level of risk
- It is a business decision and should align with strategic and capital planning initiatives

Risk Mitigation Decisions

- Elimination of all risk is realistically impossible
- Management generally uses the most cost-effective approach and implements the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission



Risk Mitigation Options (1 of 2)

- **Options** for risk mitigation depend on an organization's goals and mission
  - **Risk assumption** = accept potential risk and continue operation or implement controls to lower risk to an acceptable level
  - **Risk avoidance** = avoid risk by eliminating the cause and/or consequence
  - **Risk limitation** = limit risk by implementing controls that minimize adverse impact

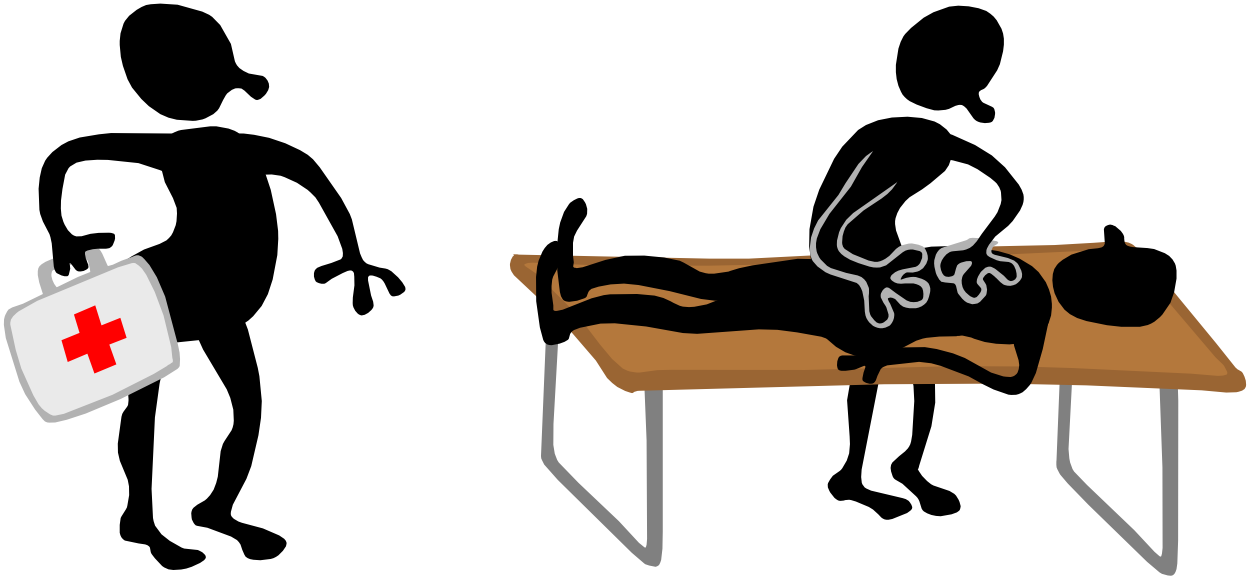
Risk Mitigation Options (2 of 2)

- **Options** continued
  - **Risk planning** = developing a risk mitigation plan that prioritizes, implements, and maintains controls
  - **Research and acknowledgement** = acknowledge vulnerability and researching corrective actions
  - **Risk transfer** = using other options, such as insurance, to compensate for the loss

Risk Mitigation

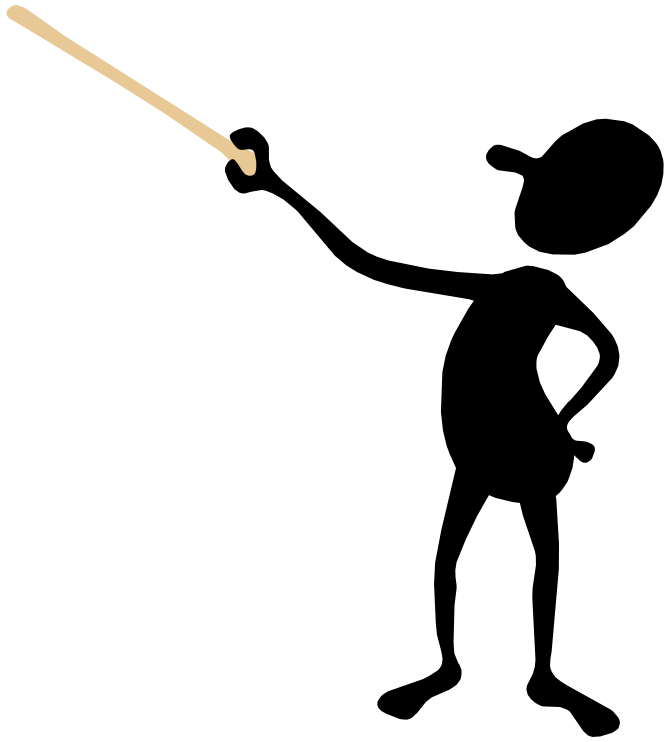
Considerations

- To make the best determination for Risk Mitigations, consider outcomes and impact



Risk Mitigation Steps

- Step 1. Determine approach to handle the risk
- Step 2. Develop risk mitigation plan
- Step 3. Implement and Document



Risk Mitigation Steps

Step 1 – Determine Approach

- Determine approach to handle the risk
    - What are the options for mitigating that risk?
- Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities

Step 1 - Determine Approach

Activities

A. Prioritize risks and identify mitigation options

B. Evaluate recommended mitigation options

C. Conduct cost-benefit analysis

Step 1 - Determine Approach

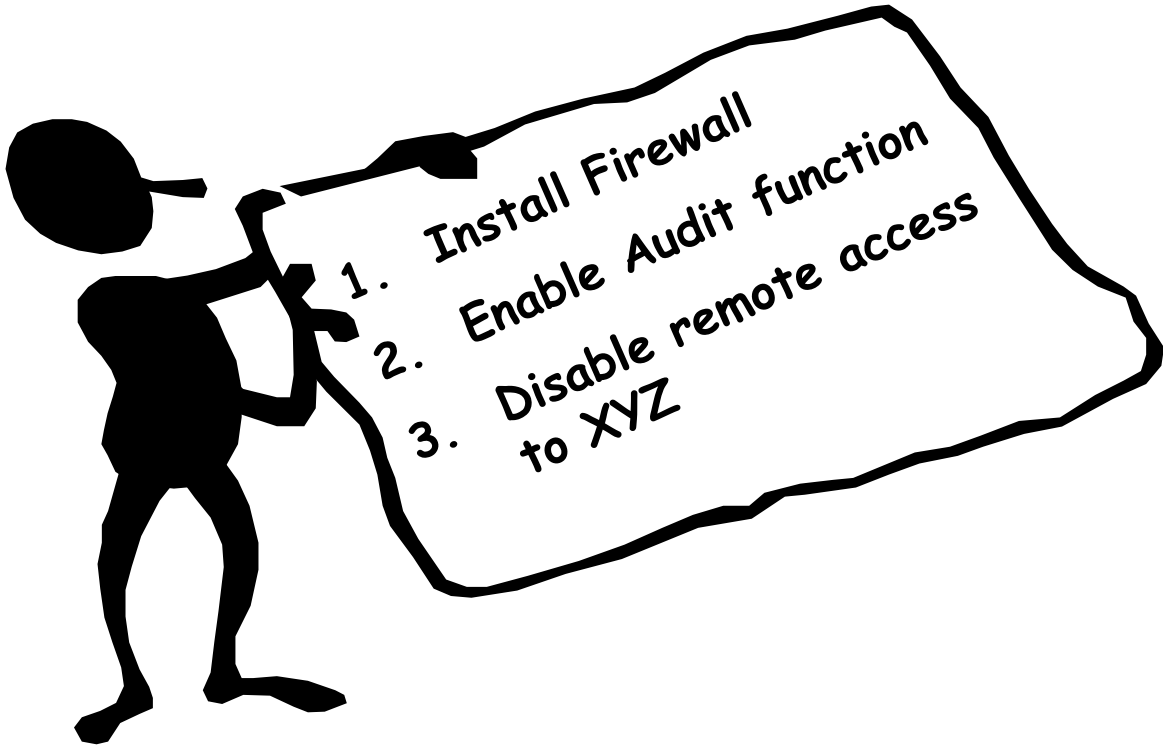
Activity A – Prioritize Risks

- From Risk Assessment Report, review the prioritized risks and mitigation options
  - Risk rankings of High are top priority
  - High priority items require immediate actions to protect organization's mission and interests

Step 1 - Determine Approach

Activity A – Prioritize Risks

- Examples of Options:
  - Actions ranking from High to Low

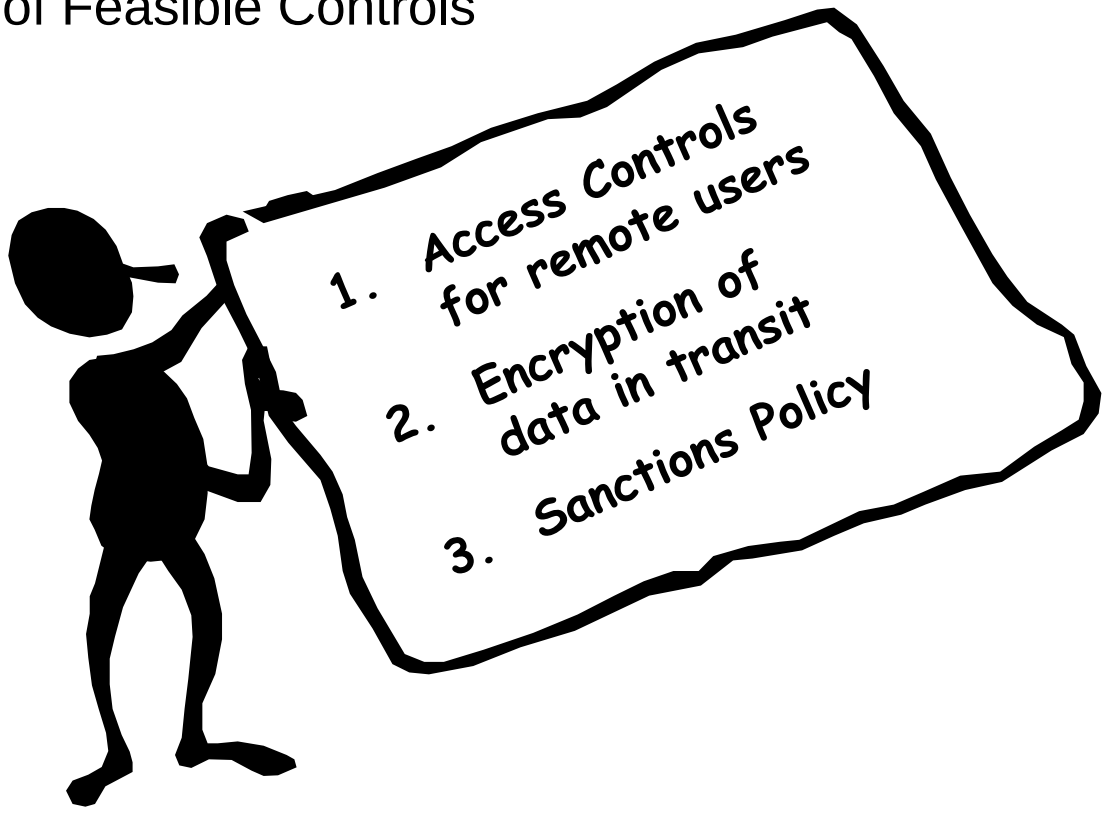


Activity B – Evaluate Recommended Control Options

- For each option, evaluate
  - Feasibility
    - Compatibility
    - User Acceptance
  - Effectiveness
    - Degree of protection
    - Level of risk mitigation

Activity B – Evaluate Recommended Control Options

- Outcome:
  - List of Feasible Controls



Activity C – Conduct Cost-Benefit Analysis

- Chose methodology: qualitative or quantitative
- Is the cost of implementing the controls justified by the reduction of the level of risk?
- Option must support the mission of the organization

Activity C – Conduct Cost-Benefit Analysis

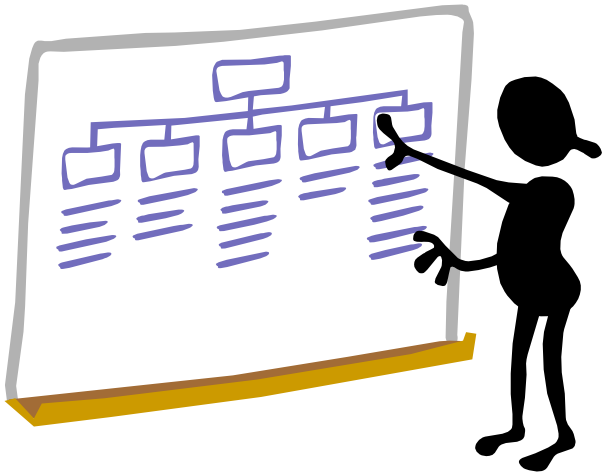
- Impact of implementing new or enhanced controls
- Impact of NOT implementing new or enhanced controls
- Estimating cost
  - Hardware and software
  - Reduced operational effectiveness if system performance is reduced for increased security
  - Implementing additional policies and procedures
  - Hiring additional staff
  - Training
  - Maintenance
- Assess the implementation costs and benefits against the system and data criticality

Activity C – Conduct Cost-Benefit Analysis

- Outcome:
  - Cost benefit analysis describing the cost and benefits of implementing or not implementing the controls
- Remember: Risk in a healthcare environment is unique with special factors
  - Life
  - Limb
  - Suffering
  - Safety

Step 2 – Develop Risk Mitigation Plan

- Develop risk mitigation plan
    - What to document on the plan?
- The strategy to mitigate risks identified. Should include a plan of action with specific tasks, responsible personnel, and dates for completion



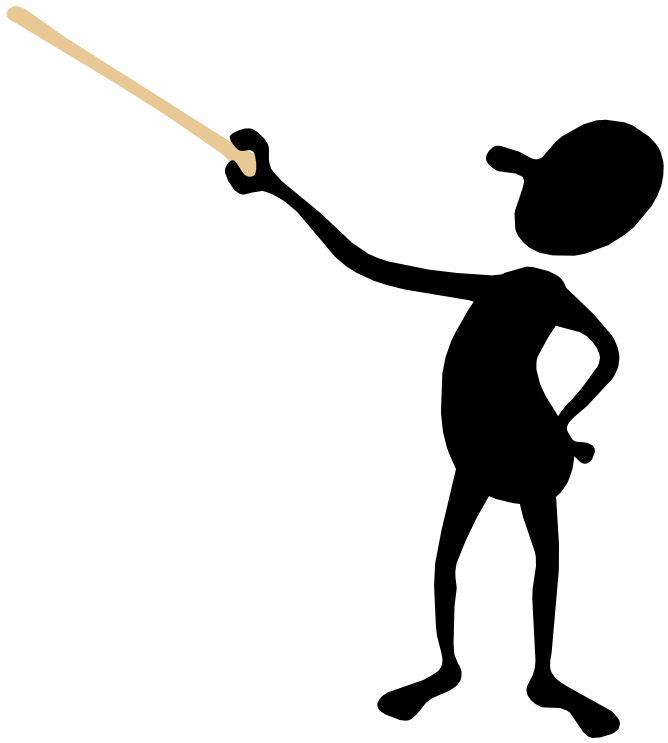
Step 2 – Develop Plan

Activities

A. Select Control

B. Assign Responsibility

C. Develop an Implementation Plan



Step 2 – Develop Plan

Activity A – Select Controls

- Select controls based on the cost benefit analysis and the control evaluation
- Combine controls from:
  - Administrative
  - Physical
  - Technical
- Controls ensure security for the IT systems, the data, and the organization

Step 2 – Develop Plan

Activity A – Select Controls

- Outcome:
  - List of Selected Controls

Step 2 – Develop Plan

Activity B – Assign Responsibility

- Identify appropriate personnel
  - Internal personnel or external contracting staff
  - Appropriate expertise and skill-sets
- Assign responsibility

Step 2 – Develop Plan

Activity B – Assign Responsibility

- Outcome
  - List of responsible persons

Step 2 – Develop Plan

Activity C – Develop an Action Plan

- Action Plan
  - Prioritizes the implementation actions
  - Projects start and completion dates
  - Aids and expedites the risk mitigation process

Step 2 – Develop Plan

Activity C – Develop an Action Plan

- Action Plan contains:
  - Prioritized Actions
  - Selected controls
  - Required resources
  - Lists of responsible teams and staff
  - Start date for implementation
  - Target complementation date
  - Action plan maintenance requirements

Step 3 – Implement and Document

A. Implement controls that mitigate risk by:

- Following the action plan
- Monitoring progress
- Communicating status

B. Update system security plan and related security documentation

Activity A - Implement Selected Controls

- Outcome:
  - Reduction in risk
  - Compliance with documentation requirements

- Remember: Residual Risk that is not eliminated by the implemented controls must be accepted by DAA or senior management

Summary: Risk Mitigation Steps

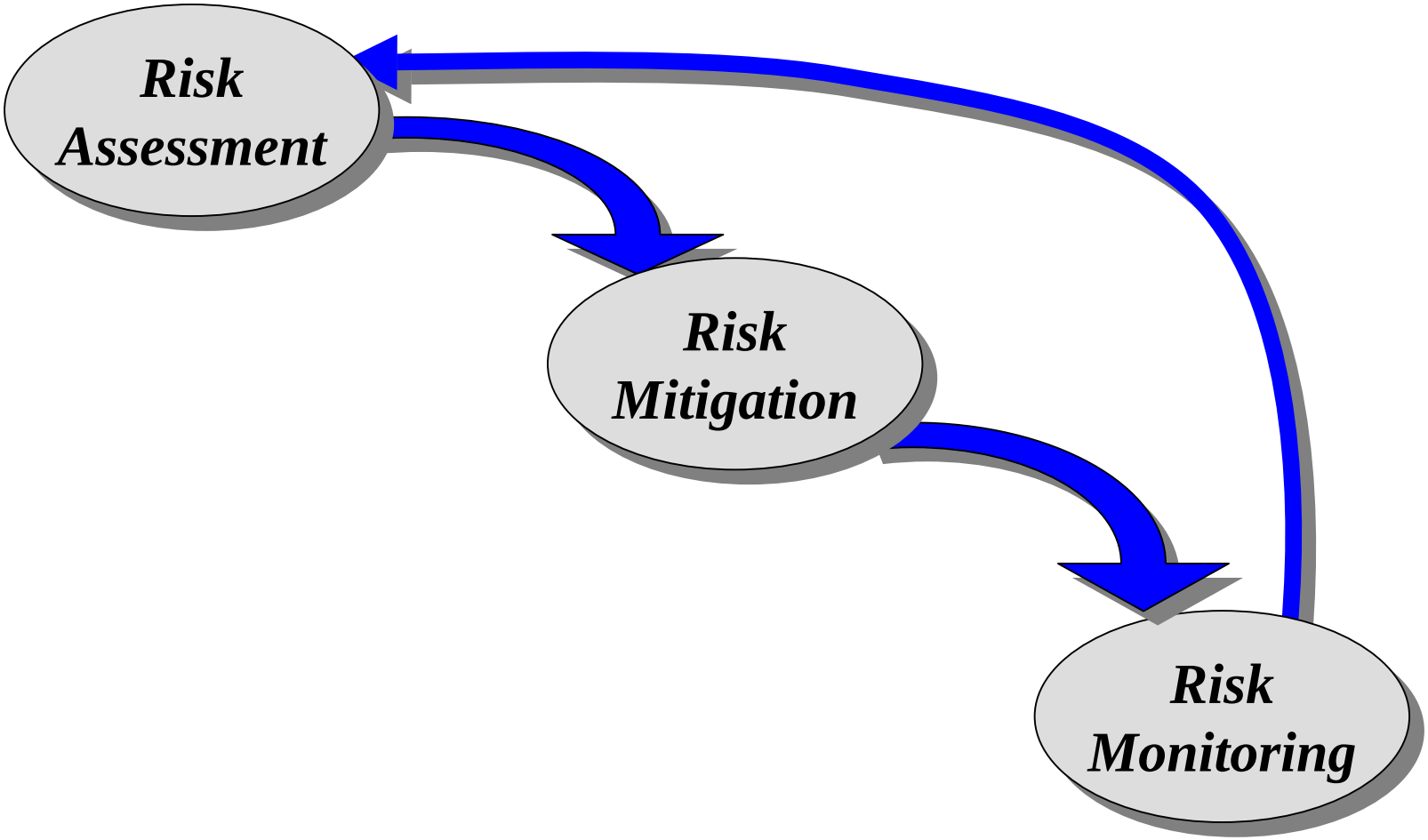
- Step 1. Determine approach to handle the risk
- Step 2. Develop risk mitigation plan
- Step 3. Implement and Document

Risk Monitoring

Objectives

- After completing this module, you should be able to:
  - Identify where risk monitoring fits in the Risk Management process
  - Describe the frequency of risk monitoring
  - Identify factors that will change the risk status of your systems

Risk Management Process



Risk Monitoring

Continual Monitoring

- Key for implementing a successful risk management program
- Necessary to keep your organization at the risk level that was deemed acceptable

Risk Monitoring

Activities

- Utilize automated tools for vulnerability scanning
- Subscribe to vulnerability list services
- Check frequently for
  - New anti-virus updates
  - Critical updates to operating systems
  - Patches

Review Schedule

- Establish the frequency of reviews of audit and system activity logs, taking into account the following factors :
  - Sensitivity of the information (EPHI)
  - Size of the facility
  - Complexity of the organization

Review Schedule

- Repeat evaluations when significant changes to the security environment are made

- Examples of changes:
  - Network expanded
  - Components changed
  - Software Applications replaced
  - Personnel rotated
  - New vulnerabilities and threats emerged

Summary

- You should now be able to:
  - Identify where risk monitoring fits in the Risk Management process
  - Describe the frequency of risk monitoring
  - Identify factors that will change the risk status of your systems

Keys for Success

- Senior management's commitment
- Full support and participation of the IT team
- Competence of the Risk Assessment team
  - Expertise of applying the risk assessment methodology to the system and the organization
  - Identification of mission risks
  - Provide cost-effective safeguards that meet the need of the organization

Keys for Success

- Awareness and cooperation of the user population
  - Follow procedures
  - Comply with implemented controls
- Ongoing evaluation and assessment of the IT related mission risks

Summary

- You should now be able to:
  - Describe risk management
  - Define threats
  - List and describe the nine-steps of the risk assessment methodology
  - Describe the risk mitigation options

Summary

- You should now be able to:
  - Define basic information security concepts
  - Describe the elements of the risk management process
  - Identify the risk management activities of the HIPAA Security Rule
  - Describe how OCTAVE and HIPAA BASICS support HIPAA compliance

Resources

- Title 45, Code of Federal Regulations, “Health Insurance Reform: Security Standards; Final Rule,” Parts 160, 162 and 164, current edition
- http://www.tricare.osd.mil/tmaprivacy/Hipaa.cfm
- privacymail@tma.osd.mil for subject matter questions
- hipaasupport@tma.osd.mil for tool related questions
- Service HIPAA security representatives

HEALTH AFFAIRS

TRICARE
Management
Activity

Please fill out your critique

Thanks!